IN THE MATTER OF THE SEARCH OF:

All computers, computer hardware, computer and digital media, and wireless telephones therein located at 3185 Sleepy Hollow Drive, Sullivan, Missouri, in the County of Franklin.

AFFIDAVIT

I, John Mark Burbridge, being duly sworn, do hereby depose and state:

Introduction

1. This affiant, John Mark Burbridge, has been employed as a Special Agent for the Federal Bureau of Investigation for approximately thirty-one (31) years and is currently assigned to investigate crimes against children. During the course of this time period, this affiant has had numerous contacts and dealings with police officers, individuals known to produce, possess and/or sell obscene material, as well as subjects known to produce, possess, distribute, and or manufacture child pornographic images and/or videos. This affiant has received training in the area of internet crimes against children. This affiant has assisted in numerous investigations and search warrants relative to the crimes of manufacturing, possessing, production and/or distributing child pornography. During my career as an agent, I have conducted numerous investigations regarding the sexual exploitation of children that involve the use of a computer. The use of a computer in these cases were violations of Title 18, United States Code, Sections 2251, 2252, and 2252A, which criminalize the production, possession, receipt, distribution and transmission of child pornography. I have been personally involved in the execution of search warrants to search residences and seize material relating to the sexual exploitation of minors. This material has included computers, computer equipment, cameras, software, and electronically stored information. During the course of my career, I have had contacts and dealings with informants, other police officers, and subjects known to possess, distribute and manufacture child pornographic images.

2. This affidavit is made in support of an application for a search warrant to search for and seize instrumentalities, fruits, and evidence of violations of Title 18, United States Code, Sections 2251, 2252, and 2252A, which criminalize, among other things, the possession and/or receipt and distribution of child pornography, and other related materials. I have probable cause to believe that contraband evidence of the above-mentioned crimes, fruits and evidence of those crimes and instrumentalists of those above-mentioned violations are located within: 3185 Sleepy Hollow Drive, Sullivan, Missouri, in the County of Franklin, hereafter referred to as "SUBJECT PREMISES." The location and items that are the subject of the search and seizure applied for in this affidavit are more specifically described in Attachments A and B.

a. The SUBJECT PREMISES to be searched is located at: 3185 Sleepy Hollow Drive, Sullivan, Missouri in the County of Franklin, within the Eastern District of Missouri. The residence is a single family ranch style home. The residence has a screened in front porch built across most of the front. The entrance is on the left

end of the enclosure. There is a red metal carport on the left side of the front of the residence. The residence has tan yellow siding with dark green shutters. There is a large shed on the left as you enter the board fence entrance of the property. A barn is further out, on the right of the residence. And more further described in an Attachment A.

b. I request authority to search the SUBJECT PREMISES, including the residential dwelling and any computers, cellular telephones, computer hardware (including peripheral input/output devices), computer software, computer related documentation found there; and seize the items specified in Attachment B, which constitutes instrumentalities, fruits, contraband, and evidence of violations of Title 18, United States Code, Sections 2251, 2252 and 2252A.

c. The statements contained in this affidavit are based on personal information, information provided to me, and information obtained through a review of reports and database records.

d. Because I submit this affidavit for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts necessary to establish probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252 and 2252A have occurred and that evidence of those violations is located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

3. This investigation concerns alleged violations of: 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt, Transportation, and Distribution; and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), Possession and Access, or Attempted Access, with Intent to View Child Pornography.

a. 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) prohibits a person from knowingly receiving, distributing or conspiring to receive or distribute any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and

b. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

4. The following definitions apply to this Affidavit and attachments hereto:

   a. Child Erotica means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.

   b. "Child Pornography," as used herein, means any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8)(A) and (C).

   c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

   d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

   e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

   f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

   g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. "Internet Service Providers" or "ISPs" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

k. "Domain Name" refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and, .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

l. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

m. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

n. "Uniform Resource Locator" or "Universal Resource Locator" or "URL" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

o. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

p. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

q. A "wireless telephone," or "mobile telephone," or "cellular telephone" is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and

moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. A wireless telephone may have wireless connection capabilities such as Wi-Fi and Bluetooth. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

r. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

s. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

CHARACTERISTICS OF INDIVIDUALS THAT DISTRIBUTE, RECEIVE AND POSSESS CHILD PORNOGRAPHY

5. Based upon my experience and training, the following traits and characteristics are generally found to exist and be true in cases involving individuals who possess child pornography:

a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, IRC (Internet Relay Chat), newsgroups, instant messaging and other similar vehicles.

d. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject

of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, videos, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

e. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices or merely on scraps of paper.

f. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft and damage their collections of illicit materials. They almost always maintain their collections in the privacy and security of their homes or other secure location. Individuals who possess and transport child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

COMPUTERS AND CHILD PORNOGRAPHY

6. I have participated in investigations of persons suspected of violating federal child pornography laws, including Title 18, United States Code, Sections 2251, 2252 and 2252A. I have also participated in various mandated and volunteer training for the investigation and enforcement of federal child pornography laws in which computers are used as the means for receiving, transmitting, and storing child pornography.

7. Computers, computer hardware, wireless telephones, and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography was formerly produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these images on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of such items was most often accomplished through a combination of personal contacts, mailings, and telephone calls.

8. The development of computers, wireless telephones and computer hardware have changed the way in which individuals interested in child pornography interact with each other, as computers and computer hardware serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

9. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. Digital cameras and wireless telephones allow images to be transferred directly onto a computer. A device known as a modem permits computers to connect to other computers through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers and wireless telephones around the world.

10. The ability of computers, computer hardware and wireless telephones to store images in digital form makes them ideal repositories for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) has grown tremendously within the last several years. These drives can store hundreds of thousands of images at a very high resolution.

11. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

12. Collectors and distributors of child pornography also utilize online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

13. As is the case with most digital technology, communications by way of computer, computer hardware and wireless telephones can be saved or stored on the devices. Storing this information can be intentional, i.e., by saving an e-mail as a file or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, Internet users generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner can often recover evidence which shows that a computer contains specific software, when the software was installed, logs regarding the usage of the software, and even some of the files which were uploaded or downloaded using the software. Such information may be maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

14. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

15. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto

opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he/she often stores it in random order and with deceptive file names. The latter requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.

16. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. Moreover, the vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. As such, it is difficult to know prior to a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

17. Most individuals who collect child pornography are sexually attracted to children, as their sexual arousal patterns and erotic imagery focus, in part or in whole, on children. The collection may be exclusively dedicated to children of a particular age/gender or it may be more diverse, representing a variety of sexual preferences involving children. Collectors of child pornography express their attraction to children through the collection of sexually explicit materials involving children, as well as other seemingly innocuous material related to children.

18. The above-described individuals may derive sexual gratification from actual physical contact with children, as well as from fantasy involving the use of pictures or other visual depictions of children or from literature describing sexual contact with children. The overriding motivation for the collection of child pornography may be to define, fuel, and validate the collector's most cherished sexual fantasies involving children.

19. Visual depictions may range from fully clothed depictions of children engaged in non-sexual activity to nude or partially nude depictions of children engaged in explicit sexual activity. In addition to child pornography, these individuals are also highly likely to collect other paraphernalia related to their sexual interest in children. This other material is sometimes referred to as "child erotica," further defined as any material relating to children that serves a sexual purpose for a given individual. "Child erotica" is broader and more encompassing than child pornography, though at the same time the possession of such corroborative material, depending on the context in which it is found, may be behaviorally consistent with the offender's orientation toward children and indicative of his/her intent. "Child Erotica" includes things such as fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, cartoons and non-sexually explicit visual images.

20. Child pornography collectors may reinforce their fantasies by taking progressive,

overt steps aimed at turning such fantasy(ies) into reality in some, or all, of the following ways: collecting and organizing their child-related material; masturbating while viewing child pornography; engaging children, online and elsewhere, in conversations, sometimes sexually explicit conversations, to fuel and fortify the fantasy; interacting, both directly and indirectly, with other like-minded adults through membership in organizations catering to their sexual preference for children, thereby providing a sense of acceptance and validation within a community; gravitating to employment, activities and/or relationships which provide access or proximity to children; and frequently persisting in the criminal conduct even when they have reason to believe the conduct has come to the attention of law enforcement. These are need driven behaviors to which the offender is willing to devote considerable time, money, and energy in spite of risks and contrary to self-interest.

21. Child pornography collectors almost always maintain and possess their material(s) in the privacy and security of their homes or some other secure location, such as their vehicle(s), where it is readily available. The collection may include sexually explicit or suggestive materials involving children, such as photographs, magazines, narratives, motion pictures, video tapes, books, slides, drawings, computer images or other visual media. The collector is often aroused while viewing the collection and, acting on that arousal, he/she often masturbates, thereby fueling and reinforcing his/her attraction to children.

22. Due to the fact that the collection reveals the otherwise private sexual desires and intent of the collector and represents his most cherished sexual fantasies, some collectors rarely dispose of the collection. The collection may be culled and refined over time, but the size of the collection tends to increase. Individuals who use a collection in the seduction of children or to document the seduction of children treat the materials as prized possessions and are especially unlikely to part with them. Even if a child pornography collector deletes files from his hard drive or other electronic media, a computer expert is often able to retrieve those files using computer forensic tools.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

23. I know that when a computer user saves a file to the computer's hard drive or other storage media, the system assigns the data to specific clusters or locations on the media, which are then reserved. The event may also be recorded in other files on the computer such as .dat and link files. If the user later deletes a file, the data is not actually erased, but rather the system marks those previously reserved clusters as once again being available for use. The original data is still intact on the media. The data is recoverable until it is overwritten either by the use of a "wiping" program or when new files are saved and assigned the same clusters. The process of overwriting may not eradicate the entire file, leaving portions available for recovery. It is therefore possible that the data can be recovered for an extended period of time even after the file itself has been "deleted." It is not unusual for this data to remain on the computer for months or years later. Until the data is overwritten, it is still in a recoverable state.

24. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to

be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals and others) can store the equivalent of thousands of pages of information. Especially, when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure, which is designed to protect the integrity of the evidence, and to recover even hidden, erased, compressed, password protected or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

25. To fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

26. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime, and should all be seized as such.

27. I know that cellular telephones are no longer much different from computers. They store voice mail messages, names, telephone numbers, addresses, sent and received text messages, images and videos on their digital memory.

28. A thorough search of digital media, to include the cellular telephones, for evidence of instrumentalities of a crime commonly requires a qualified expert to conduct the search in a laboratory or other controlled environment. This is true for the following reasons:

a. Searching digital media is a highly technical process, which require specific expertise and specialized equipment. There are so many types of digital media in

use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with personnel who have specific expertise in the type of digital media that is being searched.

b. Searching digital media requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password protected data. Since such data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential in conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

SEARCH METHODOLOGY TO BE EMPLOYED

29. The search procedure of electronic data contained in computer, wireless telephones, computer hardware, computer software, and/or memory storage devices may include the following techniques (NOTE: The following is a non-exclusive list, as other search procedures may be employed):

a. Examination of all of the data contained in such computers, computer hardware, wireless telephones, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as listed in Attachment B;

b. Searching for and attempting to recover any deleted, hidden, and/or encrypted data to determine whether that data falls within the list of items to be seized as listed in Attachment A (any data that is encrypted and/or unreadable will be returned when law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. Surveying various file directories and the individual files they contain;

d. Opening files in order to determine their contents;

e. Scanning storage areas;

f. Performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or

g. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

DETAILS OF INVESTIGATION / PROBABLE CAUSE TO SEARCH SUBJECT PREMISES

30. Robert Boevingloh ("Boevingloh") is a white male, date of birth October 11, 1943. Boevingloh resides in the SUBJECT PREMISES. On December 13, 2018, Boevingloh was indicted under seal in the Eastern District of Missouri on one count of receipt of child pornography in violation of Title 18, United States Code, Section 2252A(a)(2).

31. In December 2016, a juvenile, D.S. made a spontaneous disclosure to his mother that a family friend, Boevingloh, had molested him. This was after his parents confronted him about his outbursts, grades dropping and becoming withdrawn and anti- social. D.S.'s mother confided in his school counselor, who made a call to the Child Abuse Hotline. Children's Division Investigator Nikki Breuer sent a referral to the Children's Advocacy Center.

32. On January 19, 2017, D.S.'s mother brought D.S. to the center where an interview was conducted by Forensic Interviewer Christi Leslie. During the interview, D.S. disclosed that he is fourteen years old. He said that approximately three years ago, he met Boevingloh through Boy Scouts and was taken out to dinner. After about a month, he went to Boevingloh's house to watch television and play video games.

33. D.S. stated that on more than one occasion, Boevingloh took things too far and that Boevingloh molested D.S. D.S. said that Boevingloh only touched him when he was at Boevingloh's house and they were usually watching television. D.S. described how he would be sitting close to Boevingloh on the couch. Boevingloh asked him if he felt 'okay with this?' Although D. S. said he said 'no', Boevingloh put his hand down D. S.'s shorts and underwear and touched his penis and began rubbing up and down. D.S. described how Boevingloh tried this in the lying down position, as well, and then pulled down his own pants, in D. S.'s opinion to go 'further in'. D. S. said that he told Boevingloh to stop and that he did not want him to go any further.

34. When Boevingloh tried taking D.S.'s clothes off D.S. got off the couch and went outside. Boevingloh grabbed his hand and put it down D.S.'s pants, but D. S. said he took Boevingloh's hand out.

35. When the interviewer asked D.S. if he had seen any pictures or movies of anyone without their clothes on, D.S. stated that he played video games on Boevingloh's laptop. He said he saw pictures of Boevingloh and his genitalia. D.S. said that he also observed a picture of Boevingloh and his horse. In the picture Boevingloh was holding open the horses' anus. In another picture, D.S. described how he saw another naked adult male tied up in the barn and Boevingloh was penetrating the male.

36. At approximately 8:40 a.m., on February 2, 2017, Franklin County Detective Theresa Lustwerk was taking photographs of the SUBJECT PREMISES in preparation for a Missouri state search warrant. Boevingloh came out of the residence wanting to know why the Detective was taking pictures of his house. Detective Lustwerk made contact with Boevingloh. In the conversation, Detective Lustwerk asked Boevingloh if he was still volunteering with the

Boy Scouts. Boevingloh acknowledged that he knows D.S. and that he has spent the night on the couch there a couple of times. When asked if he would like to come to the Sheriff's Office to speak about allegations made by D.S., Boevingloh said that he didn't have anything to hide, but thought he should call his son, who is an attorney.

37. On February 7, 2017, Detective Lustwerk obtained a Missouri search warrant for the SUBJECT PREMISES for evidence of the crimes of bestiality and child pornography.

38. On February 8, 2017, Boevingloh and his attorney, David Bruns, met with Detective Lustwerk to discuss the allegations by D.S. In the interview, Boevingloh said that D.S.'s mom and uncle did lawn care for him. At one point, they brought D.S. along and they talked about boy scouts. Boevingloh said that he offered to take D.S. to scouts on Monday nights to help out D.S.'s family. He said that D.S. would call him and talk about things other than scouts. D.S. asked if he could come over to Boevingloh's house. He told D.S. to get permission from his mother. When D.S. came over, they would do things like go to the park, hike, pet the animals on his farm, or watch TV. Boevingloh said that he took D.S. to scouts for about six months. During that time, he estimated that D.S. asked three times to spend the night. Boevingloh always had D.S.'s mother's permission and this occurred on a Friday or Saturday night. D.S. slept on the couch. Boevingloh slept in his own room. Boevingloh insisted in not knowing where D.S. came up with the things that he said he saw on the computer. He said that if D.S. was watching television, he would be in his room on the computer. Boevingloh denied ever speaking to D.S. in a sexual manner and described D.S.'s description of things as 'bizarre'. Boevingloh said that he never put his hand down D.S.'s pants and D.S. never put his hand down Boevingloh's pants. He insisted that nothing like that ever happened and has no idea why D.S. would be saying anything like approximately three years later with no contact. Boevingloh did admit that they lay on the couch together full clothed to watch TV. He insisted there was never any sexual contact between the two of them. He began s~~igating~~ stating that D.S. had 'some issues'. Boevingloh brought up that D.S. admitted to having hurt a few small animals and Boevingloh was appalled by D.S.'s actions. He also talked about how D.S. told him of some physical abuse from his step-father. After this, Boevingloh said that he made excuses to stop taking D.S. to scouts. The family moved shortly after that. They and Boevingloh parted on good terms. He last saw them shortly before they left the area and moved to Steelville.

39. On February 8, 2017, following the interview, Detective Lustwerk executed the Missouri state search warrant at the SUBJECT PREMISES and seized a Hadron computer tower, a Seagate hard drive, Lexar removable hard drive, an AT&T Tracfone model 2222, four compact discs, a yellow floppy disc and a HTC cell phone. The seized items were taken to the Regional Computer Crimes Education and Enforcement Group (RCCEEG) to be examined.

40. A forensic examination of the hardrive of the Hadron computer tower revealed approximately 402 images and 61 video files depicting child pornography. The examination also revealed numerous saved Skype chat logs between Boevingloh, using the username "nudefarmer2," and other individuals discussing collecting and trading child pornography, and Boevingloh's sexual attraction to young children, including D.S. The examination further revealed several video files depicting, in part, Boevingloh and another younger man engaged in sexual activity with a dog and horse. In one of these video files, dated September 22, 2012,

Boevingloh physically places the dog in position to anally penetrate the younger man. The examination also revealed several Word documents, apparently authored by Boevingloh using various aliases, including "nudefarmer" and "nudefarmer2," that contain narratives of incestuous sexual encounters, including with a four-year-old grandson. The examination recovered files indicating the use of Ares (a P2P file sharing program), Dropbox (a cloud storage program) and Skype File Transfers (an internet messaging application). The examination also revealed that the hard drive had installed the "TrueCrypt" application, which is an encryption utility that allows users to create encrypted partitions on a hard drive, that had encrypted a folder containing approximately 10 gigabytes of data. To date, law enforcement has not been able to access any encrypted data in this folder.

41. Law enforcement is also aware that, in October 2016, the Skype username "nudefarmer2," which matches the data discovered on the Boevingloh's seized computer, uploaded child pornography using Skype servers. The IP address associated with this upload resolves to Sullivan, Missouri, where the SUBJECT PREMISES are located.

42. On December 13, 2018, Boevingloh was indicted under seal on one count of receipt of child pornography in violation of Title 18, United States Code, Section 2252A(a)(2).

43. On December 17, 2018, at approximately 6:10 am, agents with the Federal Bureau of Investigation and officers with Franklin County Police Department executed an arrest warrant of Boevingloh at the SUBJECT PREMISES.

44. Before announcing their presence, agents observed through a window that Boevingloh was in a back room of the residence sitting at a desk in front of a computer.

45. Agents knocked at the door, and Boevingloh answered in underwear and a t-shirt. Boevingloh was placed under arrest. Boevingloh requested that agents retrieve his pants from the back room, and pointed agents to the room where he was previously observed sitting.

46. Agents discovered Boevingloh's pants on the back of a chair in front of a HP desktop computer. The computer was on and the screen was in plain view to agents as they retrieved Boevingloh's pants. The computer was connected to the internet and a Mozilla Firefox window entitled "Mature / younger room" was shown on the screen.

47. Below the title bar is a URL showing that the chatroom appears to be hosted by the website www.silverdaddies.com, which is a membership website that advertises itself as "THE site for dads and their younger admirers" and states on its front page: "This site is a meeting place for mature men and other men (both daddies and younger) who are interested in keeping their daddy happy and/or sexually satisfied. The site offers the possibility of having a personal ad and also features galleries (changed daily) and a chat – and its free!"

48. Agents observed on the computer screen chat room messages wherein various users appear to be seeking sexual encounters with others, including younger men. For example, one user named "David" had messaged "fit older guy for young guy hot chat and cam." Another

user named "friendly skp" had messaged "cum for dad." Another user named "Please (Melb)" had messaged "Any younger tops want to chat?"

49. Next to the HP desktop computer were various compact discs, thumb drives, and a web camera. These items were left in the SUBJECT PREMISES by law enforcement. Law enforcement had previously seized all computer devices from the SUBJECT PREMISES in February of 2017.

50. Agents also observed a stack of photos on the kitchen table that depicted nude males displaying their genitalia. Agents were not able to determine if these males are children or adults. Agents did not see all photos in the stack.

CONCLUSION

51. Based on the above information, there is probable cause to believe that 18 U.S.C. §§ 2252 and 2252A, which, among other things, make it a federal crime for any person to knowingly possess, receive, and/or distribute child pornography, have been violated, and that the property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located within 3185 Sleepy Hollow Drive, Sullivan, Missouri, in the County of Franklin, and all computers, computer hardware, computer and digital media, and wireless telephones therein.

52. Your Affiant requests authority to seize such material, specifically, that the Court issue a search warrant for SUBJECT PREMISES and all computers, computer hardware, computer and digital media, and wireless telephones therein for the items listed in Attachment B.

53. In order to prevent the compromise of this on-going investigation, affiant respectfully requests that the application, affidavit and search warrant be sealed.

54. Based upon the foregoing, I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES, more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B.

JOHN M. BURBRIDGE
Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me this 17th day of December, 2018.

NANNETTE A. BAKER
United States Magistrate Judge
Eastern District of Missouri

ATTACHMENT A

1. The SUBJECT PREMISES to be searched is located at: 3185 Sleepy Hollow Drive, Sullivan, Missouri in the County of Franklin, within the Eastern District of Missouri. The residence is a single family ranch style home. The residence has a screened in front porch built across most of the front. The entrance is on the left end of the enclosure. There is a red metal carport on the left side of the front of the residence. The residence has tan yellow siding with dark green shutters. There is a large shed on the left as you enter the board fence entrance of the property. A barn is further out, on the right of the residence.

2. The premises to be searched includes any appurtenances to the real property that is the SUBJECT PREMISES, and any storage units or outbuildings.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEARCHED FOR AND SEIZED

1. All visual depictions, including still images, videos, films, or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, and any mechanism used for the receipt or storage of the same, but not limited to:

> Any computer, computer system, cellular devices, Personal Data Assistants (PDAs), and any related peripherals, including any data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, computer compact disks, CD-ROMs, DVD, and other memory storage devices) as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

2. Computer monitors, keyboards, and computer mice.

3. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

4. Any and all computer data that would reveal the presence of malware, viruses, or malicious codes located on the computer storage media, or computer data that would indicate the lack of malware, viruses, or malicious codes.

5. Any and all documents, records, emails, logs, and Internet history (in documentary or electronic form) pertaining to the production, possession, receipt, or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, pertaining to an interest in child pornography whether transmitted or received; pertaining to the persuading, inducing, enticing, or coercing of minors to engage in prostitution or any sexual activity; or pertaining to the transfer of obscene matter to minors.

6. Any and all materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings. "Child erotica" may also include, in this context, sex aids and/or toys.

7. Any and all records, documents, invoices, and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs, and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

8. Records, documents, invoices, and materials that demonstrate use or control of an Internet Service Provider account, including paid bills as well as all records relating to the ownership or use of computer equipment and cellular phone found in the residence.

9. Documents and records regarding the ownership, possession, and/or control of the searched premises. These records shall be limited to utility bills, telephone bills, and rental agreements.

10. Any documents, records, programs or applications relating to the existence of counter-forensic programs (and associated data) that are designed to eliminate data from the computers.